Docket No.: GB920010007US1 (7161-224) **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of	:	Customer Number: 46320
	:	
Paul ABBOT	:	Confirmation Number: 9940
	:	
Application No.: 10/046,058	:	Group Art Unit: 2134
	:	
Filed: January 10, 2002	:	Examiner: T. Szymanski
	:	

For: METHOD AND APPARATUS FOR STORAGE OF SECURITY KEYS AND CERTIFICATES

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed September 7, 2006, wherein Appellant appeals from the Examiner's rejection of claims 1-34.

I. REAL PARTY IN INTEREST

This application is assigned to IBM Corporation by assignment recorded on January 10, 2002, at Reel 012503, Frame 0914.

II. RELATED APPEALS AND INTERFERENCES

Appellant is unaware of any related appeals and interferences.

III. STATUS OF CLAIMS

Claims 1-34 are pending and finally rejected in this Application. It is from the final rejection of claims 1-34 that this Appeal is taken.

IV. STATUS OF AMENDMENTS

The claims have not been amended subsequent to the imposition of the Third Office Action dated June 7, 2006 (hereinafter the Third Office Action).

V. SUMMARY OF CLAIMED SUBJECT MATTER

Referring to Figures 1 and 2 and independent claims 1 and 23, a method for storage of security keys and certificates in a data processing system is disclosed. In step 210, at least one entity (150) is provided in the form of a key or certificate for storage in a storage means (page 14, lines 18-21). In steps 240 and 250, the entity is fragmented into fragments (152, 154) of non-uniform length according to a predetermined algorithm (200) (page 14, lines 25-26). In step 260, the fragments (152, 154) are stored in the storage means (280) (page 14, line 27). In steps 270 and 280, the fragments (152, 154) of the at least one entity (150) are intermixed within the storage means (page 14, lines 27-30). Referring to claim 3, the storage means also contains random bit patterns (120) (page 10, lines 1-7). Referring to claim 5, the location of storing the fragments (152, 154) is also determined by the algorithm (200) (page 11, lines 3-5).

Referring to Figure 1 and independent claim 13, an apparatus for storage of security keys and certificates in a data processing system is disclosed. The apparatus includes a storage means (page 7, lines 19-24), at least one entity (150) in the form of a key or certificate for storage in the storage means (page 12, lines 8-16), and the entity (150) is stored in fragments (152, 154) of non-uniform length according to a predetermined algorithm (200) and fragments of the at least one entity (150) are intermixed within the storage means (page 14, lines 16-18).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-22 were rejected under the 35 U.S.C. § 101;

2. Claims 1-6, 9, 11-17, 20-28, and 31-34 were rejected under 35 U.S.C. § 102 for anticipation based upon Bahls et al., U.S. Patent No. 5,706,513;

3. Claims 7-8, 18-19, and 29-30 were rejected under 35 U.S.C. § 103 for obviousness based upon Bahls in view of Holloway, UK Patent Application Publication GB 2318486A; and

4. Claim 10 was rejected under 35 U.S.C. § 103 for obviousness based upon Bahls.

VII. ARGUMENT

THE REJECTION OF CLAIMS 1-22 UNDER 35 U.S.C. § 101

For convenience of the Honorable Board in addressing the rejections, claims 2-12 stand or fall together with independent claim 1, and claims 14-22 stand or fall together with independent claim 13.

On page 2 of the Third Office Action, the Examiner asserted the following with regard to the claims:

> The claimed invention is directed to non-statutory subject matter. That which is claimed within the above referenced claims is not of a concrete and tangible nature. The contents of the claims are directed to an algorithm, and a storage means that is defined as a data file. Both an algorithm and a data file are not tangible since neither is contained within any concrete means but may exist solely as a non-tangible format.

With regard to the Examiner's identification of certain limitations within the claims as being directed to non-statutory subject matter (i.e., "an algorithm, and a storage means that is defined as a data file," reference is made to the paragraph spanning pages 9 and 10 of the "Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility"[1] (hereinafter "Interim Guidelines), which is reproduced below:

> Finally, when evaluating the scope of a claim, every limitation in the claim must be considered. USPTO personnel may not dissect a claimed invention into discrete elements and then evaluate the elements in isolation. Instead, the claim as a whole must be considered. See, e.g., Diamond v. Diehr, 450 U.S. 175, 188-89, 209 USPQ 1, 9 (1981) ("In determining the eligibility of respondents' claimed process for patent protection under § 101, their claims must be considered as a whole. It is inappropriate to dissect the claims into old and new elements and then to ignore the presence of the old elements in the analysis. This is particularly true in a process claim because a new combination of steps in a process may be patentable even though all the constituents of the combination were well known and in common use before the combination was made.").

As readily apparent from the Examiner's own comments, the Examiner did not consider the scope of the claims, as a whole, as required. Instead, the Examiner has improperly focused on individual elements of the claims without regard to the entire claim.

Claims 13-22

Although claims 1-12 are directed to a method, Appellant notes that claims 13-22 are directed to an apparatus, and on this basis, without the need for further argument, claims 13-22 are directed to statutory subject matter. In the decision of In re Warmerdam,[2] the Court concluded that the method claims recited in claims 1-4 "[involve] no more than the manipulation of basic mathematical constructs, the paradigmatic 'abstract idea.'" The Court then sustained the rejection of claims 1-4 under 35 U.S.C. § 101.

[1] Official Gazette Notices, November 22, 2005.

[2] 3 F.3d 1354, 31 USPQ2d 1754 (Fed. Cir. 1994).

However, the Court noted that claim 5 of the same application recited "[a] machine having a memory which contains data representing a bubble hierarchy generated by the method of any of Claims 1 through 4." With regard to this claim, the Court stated that "[c]laim 5 is for a machine, and is clearly patentable subject matter" despite the prior finding that the method being performed by the machine was non-statutory subject matter. Therefore, since claims 13-22 are directed to an apparatus (i.e., a machine), then claims 13-22 are directed to statutory subject matter within the meaning of 35 U.S.C. § 101.

In State Street Bank and Trust Company v. Signature Financial Group, Inc.,[3] the court set forth the criteria for establishing statutory subject matter under 35 U.S.C. § 101 as follows:

> The question of whether a claim encompasses statutory subject matter should not focus on which of the four categories of subject matter a claim is directed to —process, machine, manufacture, or composition of matter—but rather on the essential characteristics of the subject matter, in particular, its practical utility. Section 101 specifies that statutory subject matter must also satisfy the other "conditions and requirements" of Title 35, including novelty, nonobviousness, and adequacy of disclosure and notice. See In re Warmerdam, 33 F.3d 1354, 1359, 31 USPQ2d 1754, 1757-58 (Fed. Cir. 1994). For purpose of our analysis, as noted above, claim 1 is directed to a machine programmed with the Hub and Spoke software and admittedly produces a "useful, concrete, and tangible result." Alappat, 33 F.3d at 1544, 31 USPQ2d at 1557. This renders it statutory subject matter, even if the useful result is expressed in numbers, such as price, profit, percentage, cost, or loss.

Thus, as articulated above, the test for determining whether subject matter is patentable under 35 U.S.C. § 101 involves deciding if the subject matter produces a "useful, concrete, and tangible result."

[3] 149 F.3d 1368, 47 USPQ2d 1596 (Fed Cir. 1998).

Appellant has established utility

A discussion of the procedural considerations regarding a rejection based upon lack of utility (i.e., 35 U.S.C. § 101) is found in M.P.E.P. § 2107.02. Specifically, M.P.E.P. § 2107.02(I) states that:

> regardless of the category of invention that is claimed (e.g., product or process), an applicant need only make one credible assertion of specific utility for the claimed invention to satisfy 35 U.S.C. 101 and 35 U.S.C. 112

In the paragraph spanning pages 6 and 7 of Appellant's disclosure and within the "Background of the Present Invention" section, Appellant stated the following:

> The core of this idea is to fragment the bytes of the keys stored in a file store, making it more difficult to identify which bytes constitute a particular key, thus removing the key's identifying pattern from the file store. This can be achieved by fragmenting a key into a number of variable length pieces which are then scattered throughout the file. The pieces of one key can be intermixed with pieces from other keys. Random bit patterns can also be added to the file to make key identification more difficult. An algorithm is used to fragment a key and to recombine it. The algorithm should only be predictable to those authorised to read the file. A simple way to do this is to use the file store pass-phrase as a basis for the algorithm.

Appellant, therefore, has asserted a credible utility. As noted in M.P.E.P. § 2107.02(III)(A), the Court of Customs and Patent Appeals in In re Langer[4] stated the following:

> As a matter of Patent Office practice, a specification which contains a disclosure of utility which corresponds in scope to the subject matter sought to be patented must be taken as sufficient to satisfy the utility requirement of § 101 for the entire claimed subject matter unless there is a reason for one skilled in the art to question the objective truth of the statement of utility or its scope. (emphasis in original)

Since a credible utility is contained in Appellant's disclosure, the utility requirement of 35 U.S.C. § 101 (i.e., whether the invention produces a useful, concrete, and tangible result) has been met.

[4] 503 F.2d 1380, 1391 USPQ 288, 297 (CCPA 1974).

The Examiner's Response

On pages 7 and 8, the Examiner's responded to Appellant's prior arguments with regard to the Examiner's rejection under 35 U.S.C. § 101. For example, the Examiner asserted the following:

> The applicant has stated that the Board decision regarding Lundgren overcomes such a rejection, however, in Lundgren, the issue was whether methods need to be "in the technological arts" and thus be computer or machine implemented. The Board's decision (with dissents) was that the answer is no. Lundgren in no way superceded or was contrary to the decisions by the Courts in *Lowry* and *Warmerdam*.

Appellant notes that the Examiner's reliance on the decisions of In re Warmerdam[5] and In re Lowry[6] is inappropriate. Neither of these decisions support the Examiner's analysis. As noted by the Federal Circuit in the AT&T Corp. decision, the process claims at issue in In re Warmerdam "did nothing more than manipulate basic mathematical constructs" and the court's decision was founded on the basis that "taking several ideas and manipulating them together adds nothing to the basic equation." The claim to a data structure found to be nonstatutory subject matter in In re Warmerdam did not just involve the manipulation of a data structure. Instead, the claim was to a data structure, per se. Specifically claim 6 recited "[a] data structure generated by the method of any of Claims 1 through 4." Since the Appellant's present invention neither manipulates "basic mathematical constructions" nor claims a data structure, per se, then Appellant respectfully submits that the Examiner has inappropriately relied upon In re Warmerdam to support the Examiner's analysis.

The Examiner's citation of In re Lowrey is also inappropriate. In this decision, while discussing the prior proceedings before within the U.S. Patent Office, the Federal Circuit noted

[5] 33 F.3d 1354, 31 USPQ2d 1754 (Fed. Cir. 1994).
[6] 33 F.3d 1579, 32 USPQ2d 1031 (Fed. Cir. 1994).

that "[t]he Board reversed the 35 U.S.C. Section 101 rejection" since the claims, which were "directed to a memory containing stored information, as a whole, recited an article of manufacture." Despite referring to this rejection, the Federal Circuit did not address the issue of statutory subject matter under 35 U.S.C. § 101. As such, the Board's reversal of the Examiner's rejection of the claims under 35 U.S.C. § 101 was left standing. However, the Federal Circuit addressed the concept of a data structure within a memory with regard to an obviousness rejection and held the following:

> In short, Lowry's data structures are physical entities that provide increased efficiency in computer operation. They are not analogous to printed matter. The Board is not at liberty to ignore such limitations.

As noted above, Appellant's present invention is not directed to a data structure, per se. Therefore, Appellant submits that the Examiner has inappropriately relied upon In re Lowrey to support the Examiner's analysis.

The Examiner further asserted the following:

> To be patent-eligible, functional descriptive material must still be claimed in combination with a hardware element (e.g., an appropriate computer readable medium) so as to become a component of a computer and enable the functionality to be realized to produce a practical application when executed.

The Examiner, however, has failed to cite to case law, or even a passage in the Interim Guidelines, that supports this assertion.

Notwithstanding the Examiner's assertion to the contrary, There is no requirement that a method, which can be performed by a computer, must be claimed in combination with a hardware element. The U.S. Patent Office has already issued thousands, if not tens of thousands of patents, which include similar types of claims since the Federal Circuit's decision of State

Street Bank & Trust Co. V. Signature Financial Group, Inc.[7] Although issued prior the State Street Bank decision, the Examiner is referred to U.S. Patent No. 5,333,184 (hereinafter the '184 patent). Claim 1 of the '184 patent is reproduced below:

> 1. A method for use in a telecommunications system in which interexchange calls initiated by each subscriber are automatically routed over the facilities of a particular one of a plurality of interexchange carriers associated with that subscriber, said method comprising the steps of:
>
> generating a message record for an interexchange call between an originating subscriber and a terminating subscriber, and
>
> including, in said message record, a primary interexchange carrier (PIC) indicator having a value which is a function of whether or not the interexchange carrier associated with said terminating subscriber is a predetermined one of said interexchange carriers.

Upon reviewing this claim, it is readily apparent to a layman in the art that all of the method steps recited in this claim could be performed by a computer. Thus, if the Examiner's analysis of the present Third Office Action was followed at the time the application, then this claim would have been rejected under 35 U.S.C. § 101.

Appellant has referred to the '184 patent because this patent was the subject of the decision by the Federal Circuit in AT&T Corp. v. Excel Communications, Inc.[8] The conclusion of the Federal Circuit with regard to the '184 patent is "we find that the claimed subject matter is properly within the statutory scope of 101." Thus, the Examiner's implied assertion that an invention capable of being implemented in software alone is per se not directed to statutory subject matter directly contradicts the decision by the Federal Circuit that the claimed subject

[7] 149 F.3d 1368, 47 USPQ2d 1596 (Fed. Cir. 1999).

[8] 172 F.3d 1352, 50 USPQ2d 1447 (Fed. Cir. 1999).

matter recited in the '184 patent is directed to statutory subject matter. Moreover, the Examiner has failed distinguish between the present claims and the claims of the '184 patent so as to support a finding that the present claims are not directed to statutory subject matter.

Examiner inappropriately asserting that claims are directed to functional descriptive material

On page 8 of the Office Action, the Examiner asserted the following:

> Functional descriptive material (e.g., software), per se, is still non-statutory. If each of the elements of the claim would reasonably be interpreted by one of ordinary skill in the art in light of Applicant's disclosure as software, it's a system of software, per se, which is functional descriptive material, and is non-statutory.

The Examiner has a fundamental misunderstanding as to what actually constitutes nonfunctional descriptive subject matter. Nonfunctional descriptive subject matter refers, for example, to an actual, physical printout of a computer program or an actual, physical photograph. As is readily apparent from the claim language, none of the claims are directed to nonfunctional descriptive subject matter. Claims 1-12 and 13-22 are respectively directed to a method and an apparatus. For the Examiner to assert that any of these claims, as a whole, are directed to nonfunctional descriptive subject matter evidences a complete misunderstanding of the law.

THE REJECTION OF CLAIMS 1-6, 9, 11-17, 20-28, AND 31-34 UNDER 35 U.S.C. § 102 FOR ANTICIPATION BASED UPON BAHLS

For convenience of the Honorable Board in addressing the rejections, claims 15 and 25 stand or fall together with claim 3; claims 16 and 27 stand or fall together with claim 5; and claims 2, 4, 6, 9, 11-14, 17, 20-24, 28, and 31-34 stand or fall together with independent claim 1.

Prior to addressing the individual claims, Appellant respectfully submits that a theme running throughout the Examiner's rejection is that the Examiner's analysis is not based upon establishing that the Bahls identically discloses the claimed invention within the meaning of 35 U.S.C. § 102. Instead, the Examiner's analysis is based upon interpreting the limitations in the claims in an unjustifiably broad manner so as to eviscerate any meaning from these limitations. In so doing, the Examiner is then able to assert that Bahls identically disclose these limitations based upon the unreasonably broad construction of the claimed limitations.

Claims 1, 13, and 23

Independent claims 1, 13, and 23 each recite an entity "in the form of a key or certificate" and that the entity is fragmented into fragments of non-uniform length. In the statement of the rejection the Examiner referred to Fig. 7; column 3, lines 41-60; column 5, lines 33-67; and column 6, lines 1-3 of Bahls to teach these limitations. As described in column 5, lines 55-62, the data object Obj 1 is divided into N segments, and referring to Fig. 7 of Bahls, each queue record 402, 502, 602, 702, 704, 706, 708 includes: (i) the divided segment of the object and (ii) a key. Thus, Bahls distinguishes between the data object Obj 1 and a key.

The Examiner, however, has failed to disclose where Bahls teaches that the key is fragmented, as recited in the claims. Therefore, whereas the claimed invention recites that an entity (e.g., in the form of a key) is fragmented, Bahls discloses that the data object Obj 1 is segmented, which fails to identically disclose the claimed invention, as recited in claims 1, 13, and 23, within the meaning of 35 U.S.C. 102.

The Examiner's Response

In the paragraph spanning pages 8 and 9 of the Third Office Action, the Examiner responded to Appellant's arguments as follows:

> In regards to applicant's assertions against the teaching of a key, a key is simply a piece of data just as the data object of the present invention (Col 3 lines 6-9). The recitation of a data object anticipates a key, as disclosed the system of Bahls includes applications that utilize data objects just as any cryptographic application utilizes a data object such as a key and as recited (Col 1 lines 26-35, 55-67) actions taken with the data object are implementation specific and as such the system inherently provides for the data object as a key when the application denotes such a process. Furthermore, passages (Col 3 line 65 - Col 4 line 17) recite that the data object is retrieved initially via a public key, which contains a private key and subsequent portions contain further segments of such a key until the retrieved key is equivalent to the predetermined value as such denoting that portions of a key are stored with each data object and thus anticipating the claim language of the applicant. (emphasis added)

The passage underlined above (i.e., "a key is simply a piece of data just as the data object of the present invention") reflects the Examiner's desire to improperly construe the language of the claims. Limitations within claims are to be given "the full breadth of the ordinary and customary meanings attributed to them by those of ordinary skill in the art."[9] The Examiner's asserted claim construction for the term key (i.e., "simply a piece of data") does not reflect the ordinary and customary meaning for this term. A key has a specific function, and although a key could be a piece of data, the piece of data must be capable of performing this function to be considered a key. The Examiner, however, has not factually established that the asserted key (i.e., data object Obj 1) would have been recognized by one having ordinary skill in the art as being capable of performing the function of a key.

To analogize the Examiner's assertion, consider the example of a claim to a metal key for a door knob. Based upon the Examiner's analysis, the Examiner's would assert that any strip of metal could identically disclose the claimed metal key since a metal key is simply a strip of

[9] Ferguson Beauregard/Logic Controls et al. v. Mega Systems, LLC et al., 350 F.3d, 1327, 69 USPQ2d 1001 (Fed. Cir. 2003).

metal. Appellant respectfully submits that one having ordinary skill in the art would not consider a plain strip of metal to identically disclose a metal key just as one having ordinary skill in the art would not consider that the data object Obj 1 of Bahls identically discloses the claimed key.

With regard to the Examiner's assertion that "the system inherently provides for the data object as a key when the application denotes such a process," Appellant respectfully submits that the Examiner's reliance upon the doctrine of inherency is misplaced. Inherency may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient to establish inherency.[10] To establish inherency, the extrinsic evidence must make clear that the missing element or function must necessarily be present in the thing described in the reference, and that the necessity of the feature's presence would be so recognized by persons of ordinary skill.[11] Furthermore, reference is made to ex parte Schricker,[12] in which the Honorable Board of Patent Appeals and Interferences stated the following:

> However, when an examiner relies on inherency, it is incumbent on the examiner to point to the "page and line" of the prior art which justifies an inherency theory. Compare, In re Rijckaert, 9 F.3d 1531, 1533, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993) (when the PTO asserts that there is an explicit or implicit teaching or suggestion in the prior art, it must indicate where such a teaching or suggestion appears in the prior art); In re Yates, 663 F.2d 1054, 107, 211 USPQ 1149, 1151 (CCPA 1981).

The Examiner did not discharge that burden of indicating where the Examiner's assertion that the system necessarily provides for the data object as a key when the application denotes such a

[10] In re Rijckaert, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993) (reversed rejection because inherency was based on what would result due to optimization of conditions, not what was necessarily present in the prior art); In re Oelrich, 666 F.2d 578, 581-82, 212 USPQ 323, 326 (CCPA 1981).

[11] Finnegan Corp. v. ITC, 180 F.3d 1354, 51 USPQ2d 1001 (Fed. Cir. 1999); In re Robertson, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999); Continental Can Co. USA v. Monsanto Co., 20 USPQ 2d 1746 (Fed. Cir. 1991); Ex parte Levy, 17 USPQ2d 1461 (BPAI 1990).

[12] 56 USPQ2d 1723, 1725 (BPAI 2000).

process appears in the prior art. Thus, the Examiner has not established that this limitation is inherently disclosed by Bahls.

The Examiner's reference to column 3, line 65 through column 4, line 17 also does not identically disclose the claimed key. For ease of reference, this citation is reproduced below:

> To retrieve a data object from the shared queue 104, an application (called the retrieving application for reference purposes; the retrieving application and the storing application may be the same or different) uses the public key to retrieve the 1st segment of the data object from the ready queue 106. The data object is locked by the retrieving application at this point. Once the 1st segment is retrieved, the retrieving application determines if there are any additional segments. This is done by checking the private key. If the private key is not equal to the predetermined value (i.e., zero), additional segments exist. The private key is then used to locate these segments on the staging queue 108. The staging queue 108 is a first-in first-out queue for each private key. That is, for a given private key, the staging queue 108 returns the segments having that private key in the order in which they were stored in the staging queue 108. Accordingly, the additional segments of the data object are returned to the retrieving application in the order in which these segments were stored in the staging queue 108.

Upon reviewing this passage, Appellant is unable to discover any teaching that the public key or private key is fragmented into fragments of non-uniform length according to a predetermined algorithm, as recited in independent claims 1, 13, and 23. Although Bahls teaches that "the staging queue 108 returns the segments having that private key in the order in which they were stored," Bahls is silent as to how these segments were fragmented.

Claims 3, 15, and 25

Claims 3, 15, and 25 each recite that "the storage means also contains random bit patterns (120)." In the statement of the rejection, the Examiner asserted that "[n]ulls as defined relate to material of no consequence, effect, or value, as such these nulls may be of any nature such as that of random bit patterns since a random bit pattern follows the same as being of no consequence, effect, or value." Appellant respectfully disagrees.

Column 5, lines 66-67 of Bahls states "the Nth segment may be padded with nulls to make its size equal to segment size." As the term "nulls" is commonly used in this context, a series of bit, each bit having the value of "0," would likely be added to the Nth segment. It is also conceivable that each bit could have the value of "1." However, in each instance the series of bits added to the Nth segment would not be random (i.e., without an ordered pattern).

The Examiner's statement that a random bit pattern is the same as nulls "since a random bit pattern ... as being of no consequence, effect, or value" is in direct contrast to Appellant's disclosure. As discussed in the paragraph spanning pages 2-3 of Appellant's disclosure, "the keys to the cryptographic systems are unusual numbers with specific mathematical properties that make it possible for an attacker to identify them within the file store." However, as discussed in the paragraph spanning pages 6-7, "[r]andom bit patterns can also be added to the file to make key identification more difficult." Thus, the claimed random bit pattern does have a consequence/effect/value, which is to make the identification of the key more difficult.

The Examiner's Response

In the first full paragraph on page 9 of the Third Office Action, the Examiner responded to Appellant's arguments as follows:

> In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., bits in addition to the stored object that are random and exhibit no discernable distinction from typical data) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 968 F.2d 1181,26 USPQ2d 1057 (Fed. Cir. 1993). The applicant has stated that the recitation of nulls does not anticipate random bit patterns, however, the definition of random denotes that any value is intrinsically random and the applicant seems to be referring to data that is probabilistically not discernable from normal datum, however such language is not present within the claim language. Additionally, the applicants recitation of random bit patterns is also anticipated by the private keys that are included within the data as is well known such keys are unique and demonstrate no discernable pattern over regular data.

The passage underlined above (i.e., "the definition of random denotes that any value is intrinsically random") is another example of the Examiner improperly construing the limitations of the claims so as to read any meaning out of these limitations. If "any value is intrinsically random," as asserted by the Examiner, then non-random (i.e., ordered) values cannot exist. By inferentially asserting that non-random numbers cannot exist, the Examiner has essentially removed the modifier "random" from the claimed limitation of "random bit patterns" since all values (i.e., bit patterns) are intrinsically random. Notwithstanding the absurdity of the Examiner's assertion, the Examiner has failed to supply any factual support for the Examiner's analysis. Instead, the Examiner's assertions are based upon argument alone.

The Examiner's argument based upon "the features upon which applicant relies (i.e., bits in addition to the stored object that are random and exhibit no discernable distinction from typical data) are not recited in the rejected claim(s)" appears to be a straw man since Appellant did not specifically refer to this in Appellant's most recent response.

The Examiner's final assertion that "the applicants recitation of random bit patterns is also anticipated by the private keys that are included within the data as is well known such keys are unique and demonstrate no discernable pattern over regular data" also lacks any factual support. The Examiner stating that a particular teaching is "well known" without anything more is not sufficient to establish a rejection under 35 U.S.C. § 102. Moreover, the Examiner's comment that "private keys ... are unique and demonstrate no discernable pattern" defies common knowledge. Private keys are not random. Instead, private keys are generated using some type of specific algorithm for the purpose of being a key.

Claims 5, 16, and 27

Claims 5, 16, and 27 each recite that "the location of storing the fragments (152, 154) is also determined by the algorithm (200)" (emphasis added). By using the term "the," these claims refer back to the first instance of the term "algorithm." Thus, the algorithm recited in claims 5, 16, and 27 that determines the location of storing the fragments is also the same algorithm that determines how the entity is to be fragmented into fragments.

In the statement of the rejection, the Examiner asserted that "[a]ny implementation that resolves such an issue must then logically be composed of an algorithm," apparently intending to assert that since the segments of the object are stored, the determination of where these segments are to be stored are a result of an algorithm. This analysis, however, fails to account for the claimed limitation that the algorithm for determining the location where the fragments are to be stored is also the same algorithm that determines how the entity is to be fragmented into fragments. The algorithm (see column 5, line 59) disclosed by Bahls does not appear to determine where the fragments are stored.

The Examiner's Response

In the first full paragraph on page 10 of the Third Office Action, the Examiner responded to Appellant's arguments as follows:

> The applicant has stated "Bahls does not appear to determine where the fragments are stored", but from the disclosure of Bahls it is clear that this is exactly what the system is doing. In Bahls the data is segmented depending on the storage location since the purpose as disclosed is that the data within Bahls is too large for a single block it is segmented between several blocks thus being stored by the algorithm that segments the data object and further related to each other through the key so that the fragments may be pieced back together properly between data blocks.

The Examiner has twisted Appellant's argument. Appellant did not state that " Bahls does not appear to determine where the fragments are stored." Instead, Appellant stated that "[t]he algorithm (see column 5, line 59) disclosed by Bahls does not appear to determine where the fragments are stored "(emphasis added). Unlike the Examiner's other arguments, in which the Examiner takes a narrow claim limitation and improperly broadens the claim limitation, in this instance, the Examiner takes a very narrow argument by Appellant about what an algorithm is capable of doing and somehow broadens this argument such that Appellant is purportedly arguing that Bahls does not disclose a particular capability. As such, the Examiner has failed to directly address Appellant's argument.

THE REJECTION OF CLAIMS 7-8, 18-19, AND 29-30 UNDER 35 U.S.C. § 103 FOR OBVIOUSNESS BASED UPON THE BAHLS IN VIEW OF HOLLOWAY

For convenience of the Honorable Board in addressing the rejections, claims 7-8, 18-19, and 29-30 stand or fall together with independent claim 1.

Claims 7-8, 18-19, and 29-30 respectively depend ultimately from independent claims 1, 13, and 23, and Appellant incorporates herein the arguments previously advanced in traversing the imposed rejection of claims 1, 13, and 23 under 35 U.S.C. § 102 for anticipation based upon Bahls. The secondary reference to Holloway does not cure the argued deficiencies of Bahls. Accordingly, the proposed combination of references would not yield the claimed invention. Appellant, therefore, respectfully submits that the imposed rejection of claims 7-8, 18-19, and 29-30 under 35 U.S.C. § 103 for obviousness based upon Bahls in view of Holloway is not viable.

THE REJECTION OF CLAIM 10 UNDER 35 U.S.C. § 103 FOR OBVIOUSNESS BASED UPON BAHLS

For convenience of the Honorable Board in addressing the rejections, claim 10 stands or falls alone.

The Examiner concluded that it is well known in the art that "when a collision occurs the object is stored immediately following the occupied spot." Notwithstanding what was known or not know by one having ordinary skill in the art, the Examiner has failed to establish a prima facie case of obviousness. The Examiner has employed an "obvious to try" argument (i.e., it would have been obvious to modify Bahls since the limitation was known in the art), which is not proper. Rather, a burden is imposed upon the Examiner to identify a source in the applied prior art for each claim limitations and identify a source for the requisite realistic motivation to modify a particular reference in a particular manner to arrive at a specifically claimed invention.[13] The Examiner, however, has failed to meet this burden.

The Examiner's Response

In the first full paragraph on page 10 of the Third Office Action, the Examiner responded to Appellant's arguments as follows:

> In support of the rejection against claim 10 the article hash collision has been provided, which details "when multiple lookup keys are mapped to identical indices... hash collision occurs. The most popular ways of dealing with this are... open addressing (searching other array indices nearby for an empty space)."

The Examiner's comments notwithstanding, the Examiner has failed to set forth the requisite factual support for the motivation to modify Bahls so as to arrive at the claimed invention.

[13] Smiths Industries Medical System v. Vital Signs Inc., 183 F.3d 1347, 51 USPQ2d 1415 (Fed. Cir. 1999); In re Mayne, 104 F.3d 1339, 41 USPQ2d 1451 (Fed. Cir. 1997).

Appellant, therefore, respectfully submits that the imposed rejection of claim 10 under 35 U.S.C. § 103 for obviousness based upon the Bahls is not viable.

Conclusion

Based upon the foregoing, Appellant respectfully submits that the Examiner's rejections under 35 U.S.C. §§ 101, 102, 103 based upon the applied prior art is not viable. Appellant, therefore, respectfully solicits the Honorable Board to reverse the Examiner's rejections under 35 U.S.C. §§ 101, 102, 103.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due under 37 C.F.R. §§ 1.17, 41.20, and in connection with the filing of this paper, including extension of time fees, to Deposit Account 09-0461, and please credit any excess fees to such deposit account.

Date: November 7, 2006

Respectfully submitted,

/Scott D. Paul/
Scott D. Paul
Registration No. 42,984
Steven M. Greenberg
Registration No. 44,725
CUSTOMER NUMBER 46320

VIII. CLAIMS APPENDIX

1. A method for storage of security keys and certificates in a data processing system comprising:

providing at least one entity (150) in the form of a key or certificate for storage in a storage means;

fragmenting the entity into fragments (152, 154) of non-uniform length according to a predetermined algorithm (200);

storing the fragments (152, 154) in the storage means (280);

wherein fragments (152, 154) of the at least one entity (150) are intermixed within the storage means.

2. A method for storage as claimed in claim 1, wherein the storage means is a data file including a block of data (110) accommodating the entities (150).

3. A method for storage as claimed in claim 1, wherein the storage means also contains random bit patterns (120).

4. A method for storage as claimed in claim 1, wherein the step of fragmenting the entity (150), fragments the bytes of the entity (150).

5. A method for storage as claimed in claim 1, wherein the location of storing the fragments (152, 154) is also determined by the algorithm (200).

6. A method for storage as claimed in claim 1, wherein the entity (150) can be read from the storage means by using the algorithm (200) to find and recombine the fragments (152, 154) of the entity (150).

7. A method for storage as claimed in claim 1, wherein the storage means has a pass code (140) and the algorithm (200) for fragmenting uses the pass code (140).

8. A method for storage as claimed in claim 7, wherein the fragments (152, 154) are stored at locations in the storage means determined by using the pass code (140).

9. A method for storage as claimed in claim 1, wherein the method includes keeping a bit map (130) as a record of fragment locations until the storage is complete (190).

10. A method for storage as claimed in claim 1, wherein in the event that a fragment (152) has already been stored at a location required for a subsequent fragment (154), the subsequent fragment (154) is stored immediately after the existing fragment (152).

11. A method for storage as claimed in claim 1, wherein the storage means is a keystore repository.

12. A method for storage as claimed in claim 11, wherein the algorithm (200) is implemented as a keystore class.

13. An apparatus for storage of security keys and certificates in a data processing system comprising:

a storage means;

at least one entity (150) in the form of a key or certificate for storage in the storage means;

wherein the entity (150) is stored in fragments (152, 154) of non-uniform length according to a predetermined algorithm (200) and fragments of the at least one entity (150) are intermixed within the storage means.

14. An apparatus for storage as claimed in claim 13, wherein the storage means is a data file including a block of data (110) accommodating the entities (150).

15. An apparatus for storage as claimed in claim 13, wherein the storage means also contains random bit patterns (120).

16. An apparatus for storage as claimed in claim 13, wherein the location of the fragments (152, 154) is also determined by the algorithm (200).

17. An apparatus for storage as claimed in claim 13, wherein the entity (150) can be read from the storage means by using the algorithm (200) to find and recombine the fragments (152, 154) of the entity (150).

18. An apparatus for storage as claimed in claim 13, wherein the storage means has a pass code (140) and the algorithm (200) for fragmenting uses the pass code (140).

19. An apparatus for storage as claimed in claim 18, wherein the fragments (152, 154) are stored at locations in the storage means determined by using the pass code (140).

20. An apparatus for storage as claimed in claim 13, wherein a bit map (130) is kept as a record of fragment locations until the storage is complete (190).

21. An apparatus for storage as claimed in claim 13, wherein the storage means is a keystore repository.

22. An apparatus for storage as claimed in claim 21, wherein the algorithm (200) is implemented as a keystore class.

23. A computer program product for storage of security keys and certificates in a data processing system, said product comprising program instructions in machine-readable form on a medium, said instructions causing the system to perform the steps of:

providing at least one entity (150) in the form of a key or certificate for storage in a storage means;

fragmenting the entity into fragments (152, 154) of non-uniform length according to a predetermined algorithm (200);

storing the fragments (152, 154) in the storage means (280);

wherein fragments (152, 154) of the at least one entity (150) are intermixed within the storage means.

24. A computer program product for storage as claimed in claim 23, wherein the storage means is a data file including a block of data (110) accommodating the entities (150).

25. A computer program product for storage as claimed in claim 23, wherein the storage means also contains random bit patterns (120).

26. A computer program product for storage as claimed in claim 23, wherein the step of fragmenting the entity (150), fragments the bytes of the entity (150).

27. A computer program product for storage as claimed in claim 23, wherein the location of storing the fragments (152, 154) is also determined by the algorithm (200).

28. A computer program product for storage as claimed in claim 23, wherein the entity (150) can be read from the storage means by using the algorithm (200) to find and recombine the fragments (152, 154) of the entity (150).

29. A computer program product for storage as claimed in claim 23, wherein the storage means has a pass code (140) and the algorithm (200) for fragmenting uses the pass code (140).

30. A computer program product for storage as claimed in claim 29, wherein the fragments (152, 154) are stored at locations in the storage means determined by using the pass code (140).

31. A computer program product for storage as claimed in claim 23, wherein the instructions further cause the system to keep a bit map (130) as a record of fragment locations until the storage is complete (190).

32. A computer program product for storage as claimed in claim 23, wherein in the event that a fragment (152) has already been stored at a location required for a subsequent fragment (154), the subsequent fragment (154) is stored immediately after the existing fragment (152).

33. A computer program product for storage as claimed in claim 23, wherein the storage means is a keystore repository.

34. A computer program product for storage as claimed in claim 33, wherein the algorithm (200) is implemented as a keystore class.

IX. EVIDENCE APPENDIX

No evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 of this title or of any other evidence entered by the Examiner has been relied upon by Appellant in this Appeal, and thus no evidence is attached hereto.

X. RELATED PROCEEDINGS APPENDIX

Since Appellant is unaware of any related appeals and interferences, no decision rendered by a court or the Board is attached hereto.